20120890.0

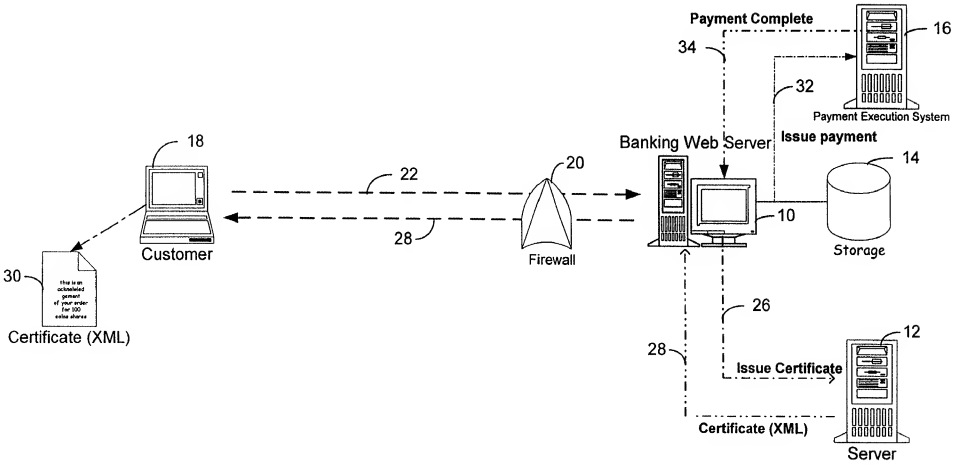


FIG. 1

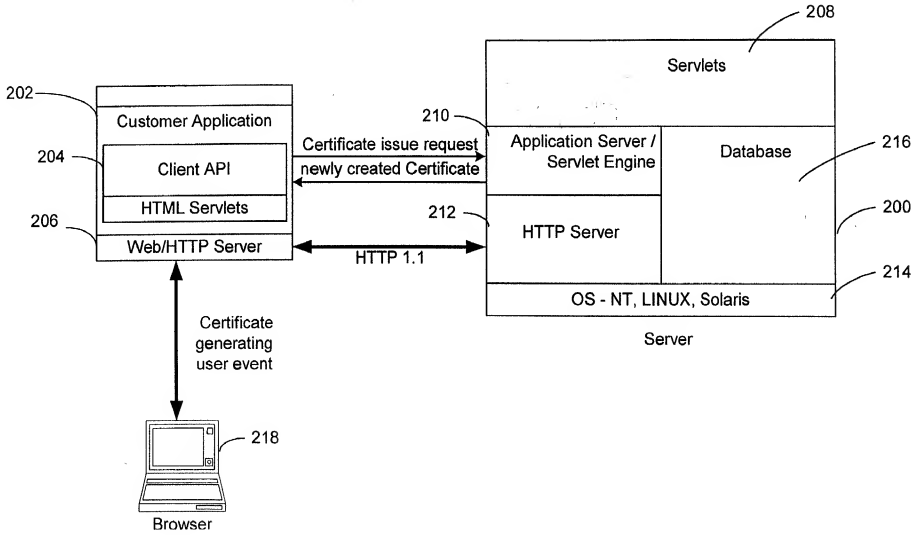
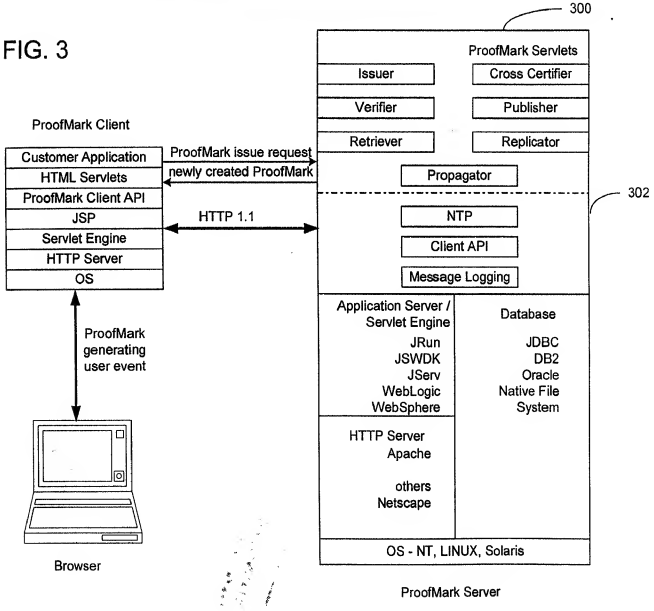

208
Servlets
202
Customer Application
210
Application Server / Servlet Engine
Database
216
204
Client API
Certificate issue request
newly created Certificate
HTML Servlets
206
212
HTTP Server
200
Web/HTTP Server
HTTP 1.1
214
OS - NT, LINUX, Solaris
Server
Certificate generating user event
218
Browser

FIG. 2

FIG. 3



09844066.021902

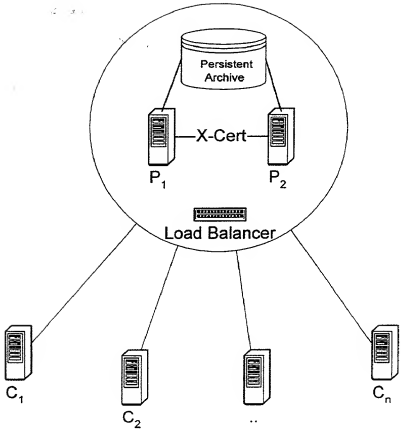


FIG. 4

Adobe Systems Inc.

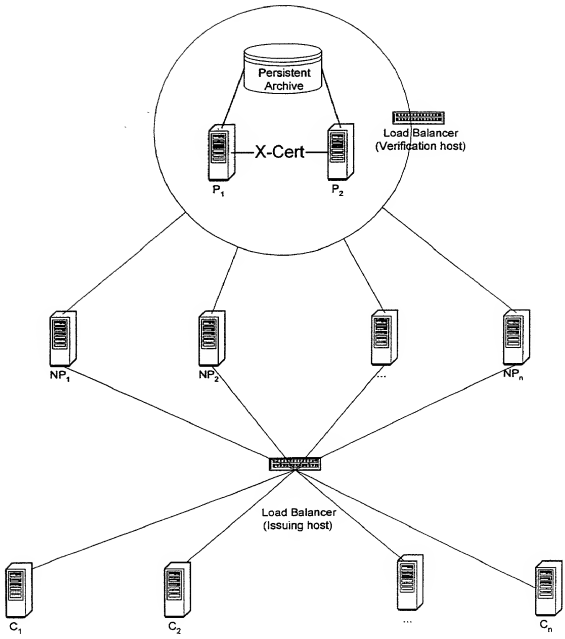


FIG. 5

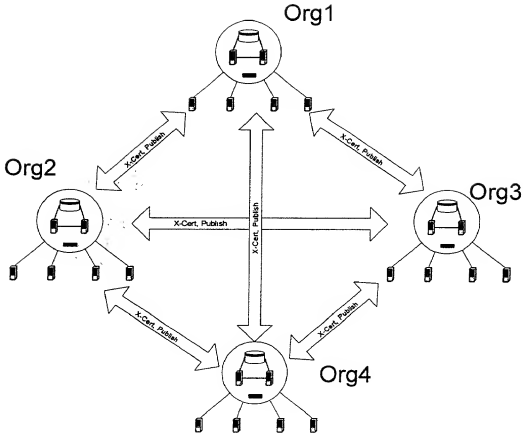

Org1
Org2
Org3
Org4
X-Cert. Publish
X-Cert. Publish
X-Cert. Publish
X-Cert. Publish
X-Cert. Publish
X-Cert. Publish

FIG. 6

20070209004860

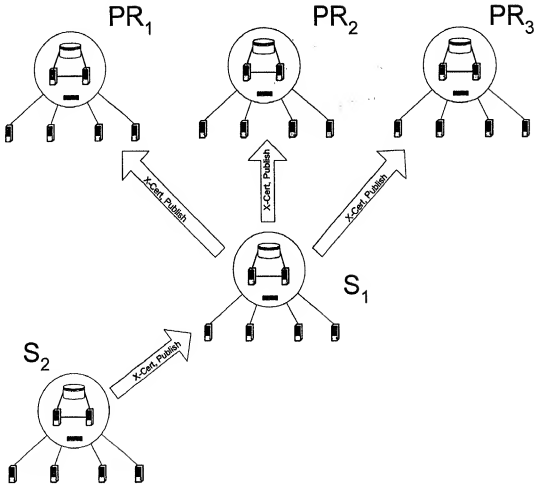


FIG. 7

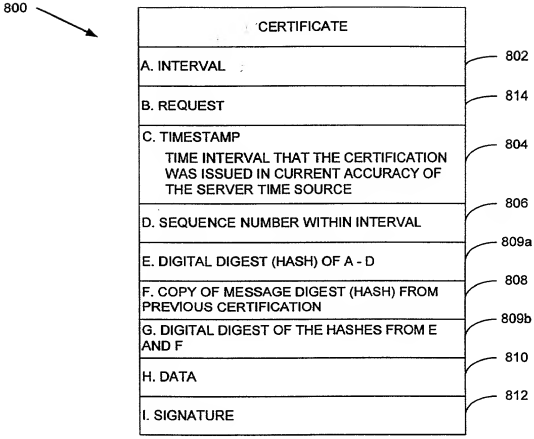

800
CERTIFICATE
A. INTERVAL
802
B. REQUEST
814
C. TIMESTAMP
TIME INTERVAL THAT THE CERTIFICATION WAS ISSUED IN CURRENT ACCURACY OF THE SERVER TIME SOURCE
804
D. SEQUENCE NUMBER WITHIN INTERVAL
806
E. DIGITAL DIGEST (HASH) OF A - D
809a
F. COPY OF MESSAGE DIGEST (HASH) FROM PREVIOUS CERTIFICATION
808
G. DIGITAL DIGEST OF THE HASHES FROM E AND F
809b
H. DATA
810
I. SIGNATURE
812

FIG. 8

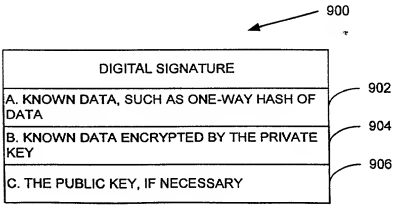

900
DIGITAL SIGNATURE
A. KNOWN DATA, SUCH AS ONE-WAY HASH OF DATA
902
B. KNOWN DATA ENCRYPTED BY THE PRIVATE KEY
904
C. THE PUBLIC KEY, IF NECESSARY
906

FIG. 9

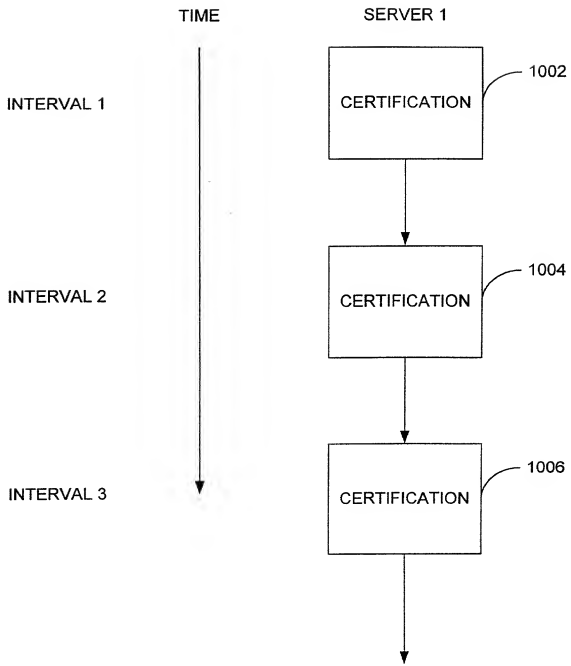

TIME
SERVER 1
INTERVAL 1
INTERVAL 2
INTERVAL 3
CERTIFICATION
CERTIFICATION
CERTIFICATION
1002
1004
1006

FIG. 10

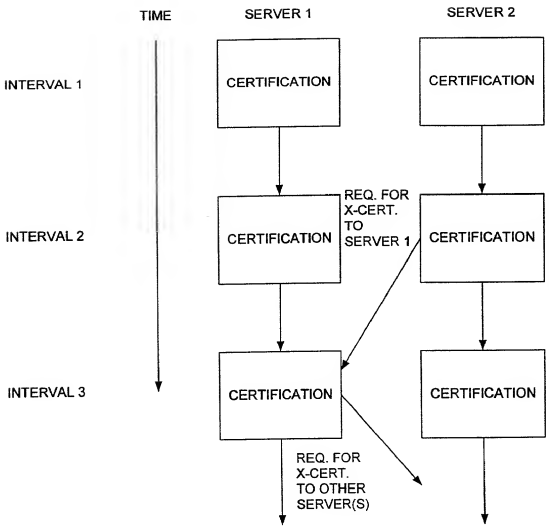

TIME
SERVER 1
SERVER 2
INTERVAL 1
INTERVAL 2
INTERVAL 3
CERTIFICATION
CERTIFICATION
CERTIFICATION
CERTIFICATION
CERTIFICATION
CERTIFICATION
REQ. FOR X-CERT. TO SERVER 1
REQ. FOR X-CERT. TO OTHER SERVER(S)

FIG. 11

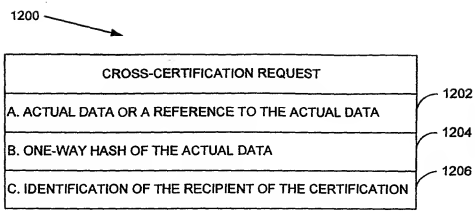

1200
CROSS-CERTIFICATION REQUEST
A. ACTUAL DATA OR A REFERENCE TO THE ACTUAL DATA
1202
B. ONE-WAY HASH OF THE ACTUAL DATA
1204
C. IDENTIFICATION OF THE RECIPIENT OF THE CERTIFICATION
1206

FIG. 12

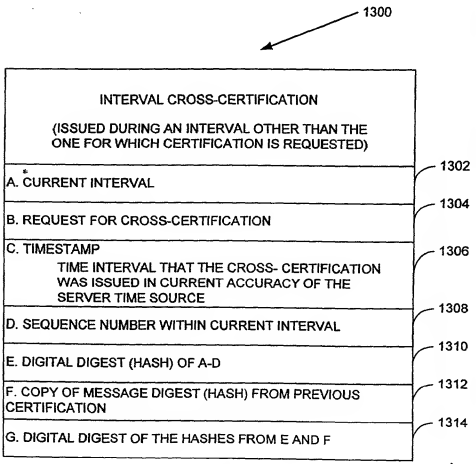

1300
INTERVAL CROSS-CERTIFICATION
(ISSUED DURING AN INTERVAL OTHER THAN THE ONE FOR WHICH CERTIFICATION IS REQUESTED)
A. CURRENT INTERVAL
1302
B. REQUEST FOR CROSS-CERTIFICATION
1304
C. TIMESTAMP
TIME INTERVAL THAT THE CROSS- CERTIFICATION WAS ISSUED IN CURRENT ACCURACY OF THE SERVER TIME SOURCE
1306
D. SEQUENCE NUMBER WITHIN CURRENT INTERVAL
1308
E. DIGITAL DIGEST (HASH) OF A-D
1310
F. COPY OF MESSAGE DIGEST (HASH) FROM PREVIOUS CERTIFICATION
1312
G. DIGITAL DIGEST OF THE HASHES FROM E AND F
1314

FIG. 13

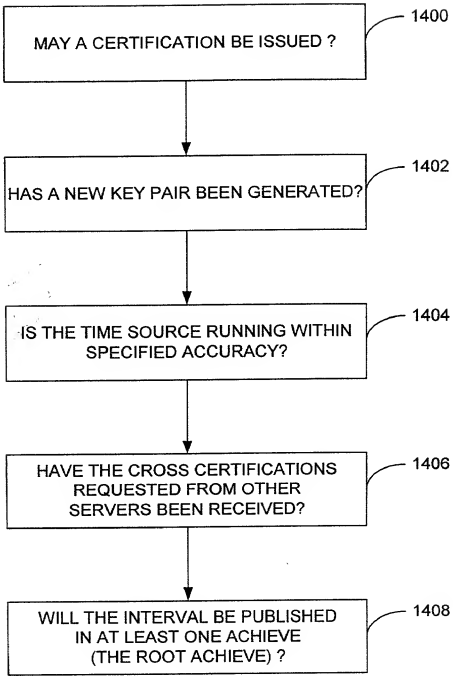

MAY A CERTIFICATION BE ISSUED ?
1400
HAS A NEW KEY PAIR BEEN GENERATED?
1402
IS THE TIME SOURCE RUNNING WITHIN SPECIFIED ACCURACY?
1404
HAVE THE CROSS CERTIFICATIONS REQUESTED FROM OTHER SERVERS BEEN RECEIVED?
1406
WILL THE INTERVAL BE PUBLISHED IN AT LEAST ONE ACHIEVE (THE ROOT ACHIEVE) ?
1408

FIG. 14

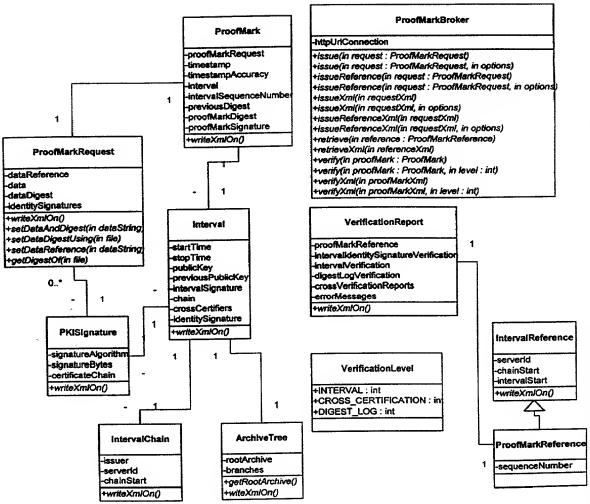

ProofMark
-proofMarkRequest
-timestamp
-timestampAccuracy
-interval
-intervalSequenceNumber
-previousDigest
-proofMarkDigest
-proofMarkSignature
+writeXmlOn()
ProofMarkBroker
-httpUrlConnection
+issue(in request : ProofMarkRequest)
+issue(in request : ProofMarkRequest, in options)
+issueReference(in request : ProofMarkRequest)
+issueReference(in request : ProofMarkRequest, in options)
+issueXml(in requestXml)
+issueXml(in requestXml, in options)
+issueReferenceXml(in requestXml)
+issueReferenceXml(in requestXml, in options)
+retrieve(in reference : ProofMarkReference)
+retrieveXml(in referenceXml)
+verify(in proofMark : ProofMark)
+verify(in proofMark : ProofMark, in level : int)
+verifyXml(in proofMarkXml)
+verifyXml(in proofMarkXml, in level : int)
ProofMarkRequest
-dataReference
-data
-dataDigest
-identitySignatures
+writeXmlOn()
+setDataAndDigest(in dataString)
+setDataDigestUsing(in file)
+setDataReference(in dataString)
+getDigestOf(in file)
Interval
-startTime
-stopTime
-publicKey
-previousPublicKey
-intervalSignature
-chain
-crossCertifiers
-identitySignature
+writeXmlOn()
VerificationReport
-proofMarkReference
-intervalIdentitySignatureVerification
-intervalVerification
-digestLogVerification
-crossVerificationReports
-errorMessages
+writeXmlOn()
PKISignature
-signatureAlgorithm
-signatureBytes
-certificateChain
+writeXmlOn()
IntervalReference
-serverId
-chainStart
-intervalStart
+writeXmlOn()
VerificationLevel
+INTERVAL : int
+CROSS_CERTIFICATION : in
+DIGEST_LOG : int
IntervalChain
-issuer
-serverId
-chainStart
+writeXmlOn()
ArchiveTree
-rootArchive
-branches
+getRootArchive()
+writeXmlOn()
ProofMarkReference
-sequenceNumber
1
0..*

FIG. 15

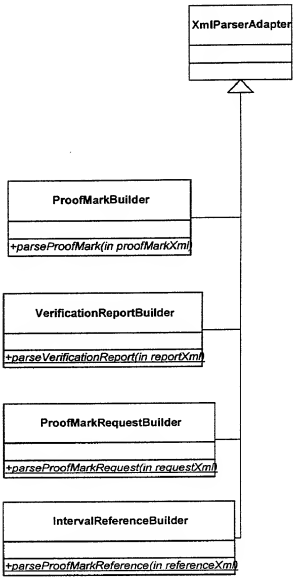

XmlParserAdapter
ProofMarkBuilder
+parseProofMark(in proofMarkXml
VerificationReportBuilder
+parseVerificationReport(in reportXml
ProofMarkRequestBuilder
+parseProofMarkRequest(in requestXml
IntervalReferenceBuilder
+parseProofMarkReference(in referenceXml

FIG. 16

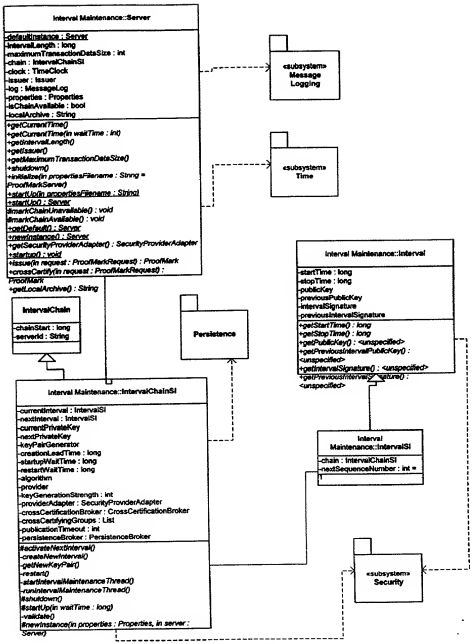

Interval Maintenance::Server
-defaultInstance : Server
-intervalLength : long
-maximumTransactionDataSize : int
-chain : IntervalChainSI
-clock : TimeClock
-issuer : Issuer
-log : MessageLog
-properties : Properties
-isChainAvailable : bool
-localArchive : String
+getCurrentTime()
+getCurrentTime(in wallTime : int)
+getIntervalLength()
+getIssuer()
+getMaximumTransactionDataSize()
+shutdown()
+initialize(in propertiesFilename : String = ProofMarkServer)
+startUp(in propertiesFilename : String)
+startUp() : Server
#markChainUnavailable() : void
#markChainAvailable() : void
+getDefault() : Server
+newInstance() : Server
+getSecurityProviderAdapter() : SecurityProviderAdapter
+startup() : void
+Issue(in request : ProofMarkRequest) : ProofMark
+crossCertify(in request : ProofMarkRequest) : ProofMark
+getLocalArchive() : String
«subsystem» Message Logging
«subsystem» Time
IntervalChain
-chainStart : long
-serverId : String
Persistence
Interval Maintenance::IntervalChainSI
-currentInterval : IntervalSI
-nextInterval : IntervalSI
-currentPrivateKey
-nextPrivateKey
-keyPairGenerator
-creationLeadTime : long
-startupWaitTime : long
-restartWaitTime : long
-algorithm
-provider
-keyGenerationStrength : int
-providerAdapter : SecurityProviderAdapter
-crossCertificationBroker : CrossCertificationBroker
-crossCertifyingGroups : List
-publicationTimeout : int
-persistenceBroker : PersistenceBroker
#activateNextInterval()
-createNewInterval()
-getNewKeyPair()
-restart()
-startIntervalMaintenanceThread()
-runIntervalMaintenanceThread()
#shutdown()
#startUp(in wallTime : long)
-validate()
#newInstance(in properties : Properties, in server : Server)
Interval Maintenance::Interval
-startTime : long
-stopTime : long
-publicKey
-previousPublicKey
-intervalSignature
-previousIntervalSignature
+getStartTime() : long
+getStopTime() : long
+getPublicKey() : <unspecified>
+getPreviousIntervalPublicKey() : <unspecified>
+getIntervalSignature() : <unspecified>
+getPreviousIntervalSignature() : <unspecified>
Interval Maintenance::IntervalSI
-chain : IntervalChainSI
-nextSequenceNumber : int = 1
«subsystem» Security

FIG. 17

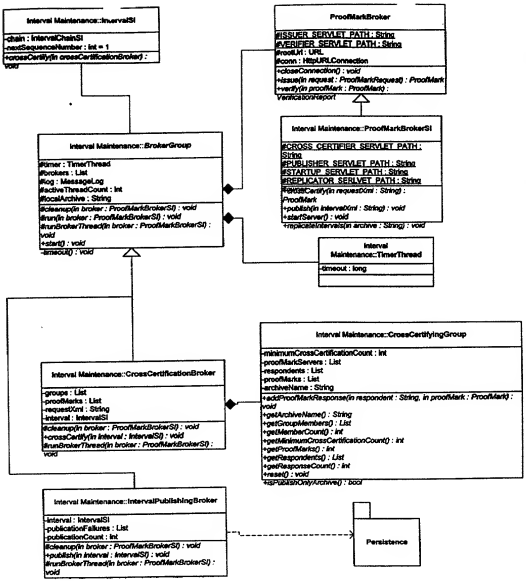

Interval Maintenance::IIntervalSI
-chain : IntervalChainSI
-nextSequenceNumber : Int = 1
+crossCertify(in crossCertificationBroker) : void
ProofMarkBroker
#ISSUER_SERVLET_PATH : String
#VERIFIER_SERVLET_PATH : String
#proofUrl : URL
#conn : HttpURLConnection
-closeConnection() : void
+issue(in request : ProofMarkRequest) : ProofMark
+verify(in proofMark : ProofMark) : VerificationReport
Interval Maintenance::ProofMarkBrokerSI
#CROSS_CERTIFIER_SERVLET_PATH : String
#PUBLISHER_SERVLET_PATH : String
#STARTUP_SERVLET_PATH : String
#REPLICATOR_SERVLET_PATH : String
#crossCertify(in requestUrl : String) : ProofMark
+publish(in intervalUrl : String) : void
+startServer() : void
+replaceIntervals(in archive : String) : void
Interval Maintenance::BrokerGroup
#timer : TimerThread
#brokers : List
#log : MessageLog
#activeThreadCount : Int
#localArchive : String
#cleanup(in broker : ProofMarkBrokerSI) : void
#run(in broker : ProofMarkBrokerSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
+start() : void
-timeout() : void
Interval Maintenance::TimerThread
-timeout : long
Interval Maintenance::CrossCertificationBroker
-groups : List
-proofMarks : List
-requestUrl : String
-interval : IntervalSI
#cleanup(in broker : ProofMarkBrokerSI) : void
+crossCertify(in interval : IntervalSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
Interval Maintenance::CrossCertifyingGroup
-minimumCrossCertificationCount : Int
-proofMarkServers : List
-respondents : List
-proofMarks : List
-archiveName : String
+addProofMarkResponse(in respondent : String, in proofMark : ProofMarkId) : void
+getArchiveName() : String
+getGroupMembers() : List
+getMemberCount() : Int
+getMinimumCrossCertificationCount() : int
+getProofMarks() : Int
+getRespondents() : List
+getResponseCount() : Int
+reset() : void
+isPublishOnlyArchive() : bool
Interval Maintenance::IntervalPublishingBroker
-interval : IntervalSI
-publicationFailures : List
-publicationCount : Int
#cleanup(in broker : ProofMarkBrokerSI) : void
+publish(in interval : IntervalSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
Persistence

FIG. 18

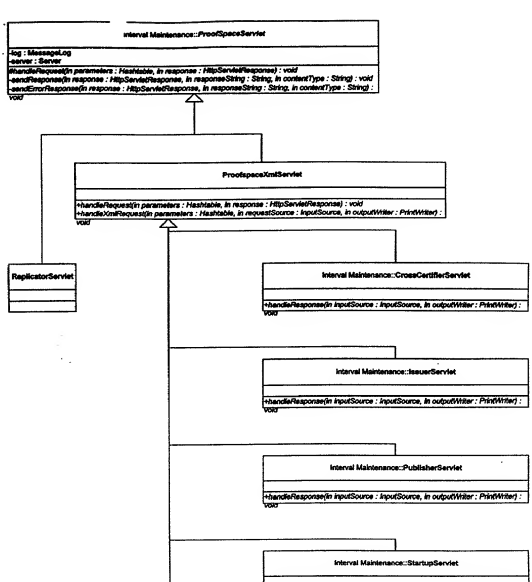

Interval Maintenance::ProofSpaceServlet
-log : MessageLog
-server : Server
#handleRequest(in parameters : Hashtable, in response : HttpServletResponse) : void
-sendResponse(in response : HttpServletResponse, in responseString : String, in contentType : String) : void
-sendErrorResponse(in response : HttpServletResponse, in responseString : String, in contentType : String) : void
ProofspaceXmlServlet
+handleRequest(in parameters : Hashtable, in response : HttpServletResponse) : void
+handleXmlRequest(in parameters : Hashtable, in requestSource : InputSource, in outputWriter : PrintWriter) : void
ReplicatorServlet
Interval Maintenance::CrossCertifierServlet
+handleResponse(in inputSource : InputSource, in outputWriter : PrintWriter) : void
Interval Maintenance::IssuerServlet
+handleResponse(in inputSource : InputSource, in outputWriter : PrintWriter) : void
Interval Maintenance::PublisherServlet
+handleResponse(in inputSource : InputSource, in outputWriter : PrintWriter) : void
Interval Maintenance::StartupServlet
+handleResponse(in inputSource : InputSource, in outputWriter : PrintWriter) : void
Interval Maintenance::VerifierServlet
+handleResponse(in inputSource : InputSource, in outputWriter : PrintWriter) :

FIG. 19

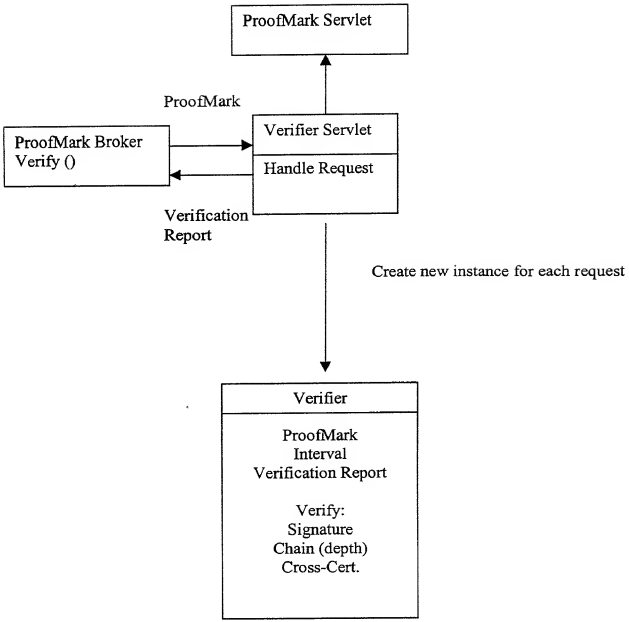

ProofMark Servlet
ProofMark
ProofMark Broker
Verify ()
Verifier Servlet
Handle Request
Verification
Report
Create new instance for each request
Verifier
ProofMark
Interval
Verification Report
Verify:
Signature
Chain (depth)
Cross-Cert.

FIG. 20

2525.2300000

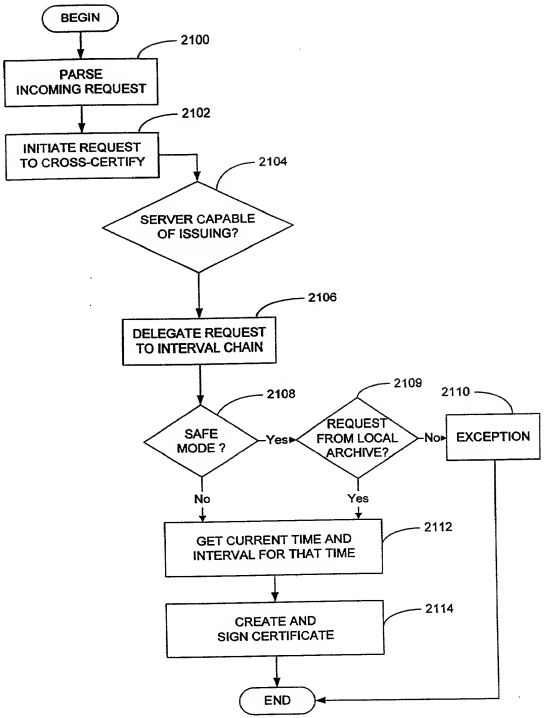


FIG. 21

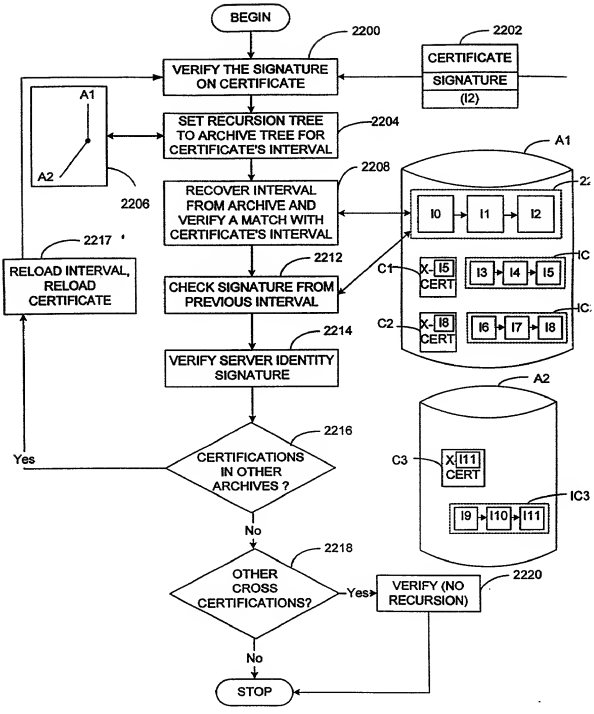

BEGIN
2200
VERIFY THE SIGNATURE ON CERTIFICATE
2202
CERTIFICATE
SIGNATURE
(I2)
A1
A2
2206
SET RECURSION TREE TO ARCHIVE TREE FOR CERTIFICATE'S INTERVAL
2204
RECOVER INTERVAL FROM ARCHIVE AND VERIFY A MATCH WITH CERTIFICATE'S INTERVAL
2208
I0
I1
I2
C1
X-I5 CERT
I3
I4
I5
C2
X-I8 CERT
I6
I7
I8
2217
RELOAD INTERVAL, RELOAD CERTIFICATE
CHECK SIGNATURE FROM PREVIOUS INTERVAL
2212
VERIFY SERVER IDENTITY SIGNATURE
2214
CERTIFICATIONS IN OTHER ARCHIVES ?
2216
Yes
No
C3
X-I11 CERT
I9
I10
I11
IC3
OTHER CROSS CERTIFICATIONS?
2218
Yes
VERIFY (NO RECURSION)
2220
No
STOP

FIG. 22